

(19)日本国特許庁（J P）(12) 公 開 特 許 公 報（A）(11)特許出願公開番号
特開2000－172548
（P2000－172548A）
(43)公開日 平成12年6月23日(2000. 6. 23)

(51)Int.Cl. ⁷	識別記号	F I	テームコト [*] (参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 H 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 M 5 B 0 6 5
12/14	3 2 0	12/14	3 2 0 B 5 B 0 8 2
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 Z 5 J 1 0 4

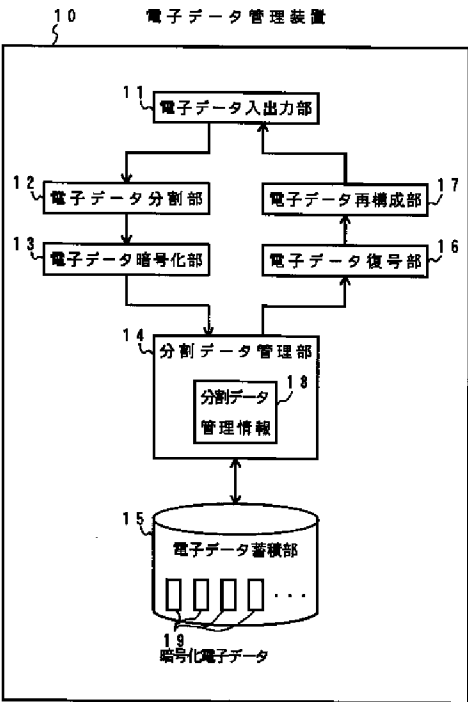
審査請求 未請求 請求項の数6 O L （全 8 頁）

(21)出願番号	特願平10－352349	(71)出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22)出願日	平成10年12月11日(1998. 12. 11)	(72)発明者	堀岡 力 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72)発明者	永田 誉興 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(74)代理人	100087848 弁理士 小笠原 吉義 （外1名）

最終頁に続く

(54)【発明の名称】 電子データ管理方法、装置およびそのプログラム記録媒体

(57) y v æ
y z s þ p
^ > ... d q f [^
d q f [^ F
z d q f [^ ~
" C P ' . d q t @ C
> " > ~ Q ' " a
C > " þ @ % d q f
14 " C ^ > d q f
" t @ C ~ ~
• Ø " f 8 • Ø B
" C " f4 " C " f
^ « ^ d9 . o
16 " C ^ > d9 C
~ 7 " C þ @ % d q f
q f [^



y i B v Z @ a - + E Q
 . Ø % v O L
 ' . d q t @ C ~
 ~ C O L ^ » f [^
 t @ C " . Ø ~
 Ø ~ C » ~ ~
 ~ C O L ' æ ^ «
 Ø O L " t @ C
 " t @ C d q f [^
 O L ~ ¥ < ‡ E % d q f [^
 @ s ‡ " Ø v O
 d q f [^ ' v O
 y i B v Z @ a - + E Q
 . Ø % v O L
 ' . d q t @ C ~
 ~ Q / " a d q f [^
 ‡ E % d q f [^ " f [^
 O L ^ » ‡ E % " f [^
 . Ø ~ C » ~ ~
 ~ C O L ' æ ^ «
 . Ø O L " t @ C
 % " t @ C d q f [^
 . Ø C O L " t @ C f
 C ‡ d q f [^ ~ ¥
 s ‡ " Ø v O L ^
 [^ ' v O
 y > Z
 y O O
 y > fl . Ø Z p " z
 ~ ‡ E % d q f [^ S
 ' ß @ x d q f
 y O O
 y] Z p z ° E C d q
 ~ ~ t @ C i [‡
 Ø B ' x ç ~ ~ t @ C
 ‡ E ~ C f [^ W ...
 ' ~ ç Ø B { C » d q
 fl " C » d q f [^
 " C ‡ ~ F E Ø p
 ^ " L fl ‡ E % d q v Z @
 " " fl E . » d q f [^
 " ç B » ' ~
 » . Ø - ~ " l f
 ' - " C s ‡ p
 ... d q f [^ ~
 B
 y O O
 y > " / ~ . Ø

p f [^ ~ ° • Ø E " ' 〇
 W Ø - B
 y O O Ø
 y E • Ø % E 〇
 ~ C d q f [^ ~ ~ 〇
 i [† E % d q f [^ ^ 〇
 > " > ~ Q ' " a " 〇
 " t @ C ~ » • d q 〇
 » æ ~ L fl • Ø B d 〇
 ~ C O L • d q t @ C 〇
 C » † E % " t 〇
 C † E % d q 〇
 y O O O T z % ~ C d q 〇
 d q t @ C i [† E % 〇
 " a " t @ C " 〇
 † E % d q f [^ " t 〇
 " t @ C ~ » • d 〇
 » æ ~ L fl • Ø B d 〇
 ^ E ^ ~ Cd Oq Lf • [d ^ q ~ t ~ @ C 〇
 < † E % d Cq " f [t ^ @ ~ CC 〇
 ~ o 〇 C » E » f 〇
 O O P R z } pQ " C { > 〇
 q f [^ y ~ O ~ O O U z " 〇
 [^ ~ Ø % • Ø E v O " 〇
 E d q f [^ C " ... - 〇
 f [^ ^ L ^ » } P R i [• 〇
 » • Ø i yX Oe O v r P Q 〇
 E C ^ y » > † E % d { q f \ 〇 z k 〇
 [^ ' P æ P { W ' ~ C d 〇
 f [^ ~ ^ " P T C " " 〇 † E % d 〇
 ~ ~ • Ø ~ i ' X 〇 • Ø E 〇
 O O P S y z O } O R O " W C z { } > P 〇 ~ C P 〇
 q f [^ [^ ' u T 〇 " ¥ < 〇
 E ~ Ø dd qq ff [[^ ^ ' 〇 u C P P 〇
 ~ ~ † E " d q q f d [q ^ f " [〇 C P R 〇
 ^ ' æ " P W f [^ ' 〇 C P T 〇
 ^ ' dæ qP fW [^ ~ 〇 C P V " 〇
 P X " • f Ø [i ^ X ' e b 〇 æ C P X 〇
 P y U O O O E X ^ z d » q 〇 f [^ ' 〇
 b v r Q ~ R ~ j • C Ø d E q f C [d 〇 q f [^ 〇
 ^ ~ fl ~ ¥ E < C • Ø fl 〇 \ % f 〇
 ~ ~ C d q f [^ ~ 〇 « " Ø f 〇
 O O P T z " { E - % " f C [^ 〇 d q f 〇
 C • Ø » E C f " % f " [C ^ ' 〇
 % a C P ' S X - " f C [O ^ L . ^ » † 〇
 % ^ X ^ P f X [j ^ C . d 〇 f [^ ~ 〇
 C E ' f i - ' " • Ø - • 〇 æ 〇
 p Ø , ~ ' C f Ø B ^ 〇

y O O P O z % C d q 〇
 % f [^ " C » " 〇
 ^ e c < - « " Ø 〇
 A - « " 〇
 y O O P P z E ° ^ » 〇
 X " " æ ~ † E ~ 〇 E 〇
 〇 fl Ø ^ » - ~ C . 〇
 Ø B E f . C / ° fi ^ 〇 B / 〇
 s / - ~ " - « Ø B / 〇
 fi ~ • Ø fi ~ " fi 〇 fi 〇
 E . C J fi ^ 〇 B fi 〇
 / fi . • Ø - ~ 〇
 " Ø B % C E ° I 〇
 v Z K v ~ • Ø % 〇
 Z v • Ø Z 〇
 y O O P Q z " f [^ 〇
 æ P W E d q f [^ P 〇
 ~ Ø ^ » d q f [^ ~ ^ 〇
 [^ P U 〇 Ø ~ ^ 〇
 C d q f [^ ~ ¥ < P V 〇

Ø - ~ " ' z k Q { 0
 y O O P U ~ C d q v Z @ 0
 " " C " # E % d q f 0
 " • Ø B } S " C Q 0
 ' u T " ¥ < f • 0
 f [^ ^ ^ » C Q P " d 0
 q f [^ ^ ^ C Q R " d 0
 f [^ ~ ¥ < C Q V " d 0
 f [^ ^ ^ æ C Q X " 0
 y O O P V z d q f [^ 0
 f [^ ^ ^ o " s / B A 0
 u p ç ~ ¶ E • 0
 Q P ~ A v P [V 0
 Ø B O P W z d q f [^ ^ 0
 y O O P W z d q f [^ ^ 0
 [^ o " Q P - fl 0
 Ø B ^ » s / ß @ ' 0
 " Q R - " C d q f [0
 # E % d q f [^ " • 0
 » Q Q Ø æ ç ~ C ^ » 0
 p ç ~ ç Ø E C } T f 0
 " C Ø ~ Z i u b 0
 R T j ^ » # E C E 0
 ~ E Ø % C e u 0
 / B O O P X z " f [^ ^ 0
 y O O P X z " f [^ ^ 0
 ~ • Ø ' f • æ " Q T 0
 C d q f [^ ~ Q T 0
 ~ • B
 y O O Q O z d q f [^ 0
 ~ Q T ~ ~ # E % ^ ç ~ 0
 ^ Q U æ Q W C " f [0
 % ^ » d q f [^ Q 0
 ^ Q V æ ç ~ # 0
 y O O Q P z } U " C { > 0
 d q f [^ ~ Q P Z 0
 f [^ o " Q P Z 0
 Ø ~ C , d q f [^ ^ 0
 ^ » i X e b v r S P 0
 Z ^ » # E % d q f [^ 0
 Q j B æ æ i X e b v r S 0
 " ¶ d q f [^ Q 0
 ~ ^ » d q f [^ Q 0
 S j B Q Q z } V " C { > 0
 y O O Q Q z } V " C { > 0
 d q f [^

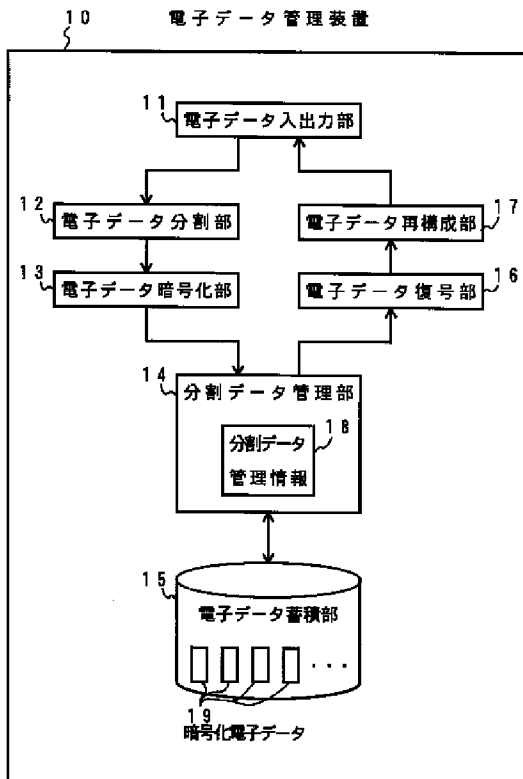
, C v # E % d q f [^ 0
 ' f • " f [^ ^ 0
 T P j C » " f [^ ^ 0
 q f [^ Q X » d q f [^ Q 0
 % ^ » d q f [^ ¥ < 0
 W ~ » O # d q 0
 æ ^ » O # d q 0
 r T S B R z k K p æ l 0
 y O O Q R z k K p æ l 0
 A v P [V C t @ C ~ 0
 f [^ i " " C t @ C ~ 0
 æ e L X g f [0
 O e L X g f [0
 ç C t @ C ~ e L X 0
 - B
 y O O Q S z G f B ^ " 0
 i ~ ' t @ C ^ v 0
 • Ø B G f B ^ o ^ 0
 v O ~ N fi • Ø 0
 ç Ø " C v Z @ v O ß 0
 Ø j f [v O ß 0
 " ç B } W i j " v O 0
 ¥ < æ C } W i a j " f [0
 v O ¥ < æ f • B 0
 v O ß fi E 0
 R " O v O ' 0
 ~ " ¥ B
 y O O Q T z W # E % e 0
 Ø E C G f B ^ " C t @ 0
 ¶ ~ ç Ø t @ C ^ 0
 t @ C " ¶ • Ø ' / 0
 V K t @ C ^ e [u 0
 o ^ • Ø B - t @ C ^ 0
 [^ ^ æ P W % " } 0
 • Ø e 0
 y O O Q U z } X C t @ 0
 Ø " f [^ ^ æ E 0
 ¥ < v f ~ ~ C ¶ 0
 C ^ » • Ø ^ fi C 0
 t @ C ... " Ø B } P 0
 ¶ Ø t @ C ... ~ C t @ 0
 ¶ w Z • Ø - 0
 " ~ ¶ • Ø - 0
 y O O Q V z t @ C " 0
 C ^ » • Ø B t @ C ... 0
 ^ I " ¶ < • Ø - 0
 C ... r b h h R [h 0

o C V c 1. Ø R C C v O ' 1
 Ø B ' r b h h R [h. "t C C ' e [u 1
 - C % c E ~] L@ fC [1
 " O - fi . Ø - "y 'O %O R T z " a t @ C 1
 " " fl 1 ... E C% < 1" C A v P [V 1
 Ø - " ' L C " 1 C v O C ß fi " K 1
 y O O Q W z C ^ » 1 T [r X ' p 1
 ^ » u b N ^ p v 1 O ß fi ~ 1
 - " ' L f [fi ^ " 1 p . Ø - " - « Ø 1
 » ß @ ' - " Ci ' LØ 1" A v P [V 1
 Ø x » E " Ø B - X E h 1 fi % C p F 1
 c / " . 1 ß fi p c ~ C t @ C A 1
 y O O Q X z E f . C. ^ Ø K 1 v " Ø - 1
 » u b N P ° Py rO bO 1
 " . Ø B T U r b g y P > ° 1 L ° z " a 1
 t @ C " < # 1 d q v Z @ a - C d q f [1
 y O O R O z " %> a - 1 L C # " d q 1
 " " Ø f [^ " ' r" bP 1
 " P o C g P ° - % »" # ' E% 1
 e r b g o Cy EO 'O R V z % C " . 1
 e 1 P r b g " - E% ' > 1 L C ^ » 1
 Ø B - E C P o C # g 1 . - 1
 " t @ C " 1 < E y O O R W z # C " 1

O O R P z 1 f [^ r 1 . Ø - 1 L C " # E 1
 C } P P f . 1 " 1 . - 1 " 1
 L N ^ j r b g æ 1 y } ° " 1
 i ' j " ~ " 1 y } P z { > P 1
 a j " " # E ^ » # 1 u T " % f 1
 E - " C d q f [^ T 1 y } Q z P { ' 1
 o C » P r b g 1 t [' 1
 b g æ P O P P O O P P 1 y } R z P { ' 1
 ~ c Ø B - E e r b 1 y } t [' 1
 r b g ' W r b g 1 y } S z { > Q 1
 " Ø " t @ C T 1 u T " % < 1
 Ø Ø R Q z b N C " 1 # 1
 } U E C Q - { % 1 ~ 1
 C L fl [ù 1 1 C » 1
 } V z . Q B t @ C ' 1
 t E C [... 1 C 1
 Ø Ø R R w d E f V ^ 1
 } " B C t @ C ' v 1
 } X z " f [^ ' t @ 1
 E f . 1 . Ø B C t 1
 } E O z " e @ C » d 1
 C " % ß @] ' 1
 C P E e 1 f [^ r b 1
 Ø Ø R B S z { E - " C a 1
 v Ø " s c C fl v 1
 O Ø d q E V ù P [V 1
 P E d q f [1 " Ø - 1

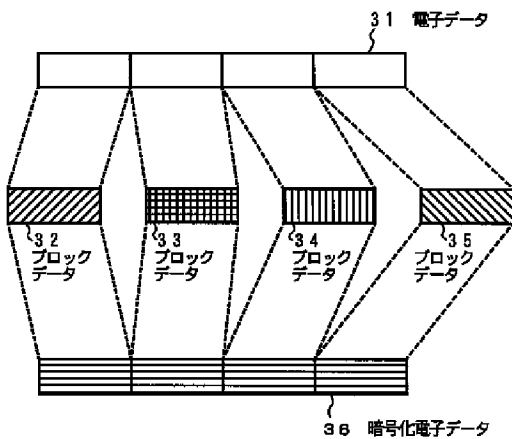
P Q R d q f ["
 P R Q d q f [〃
 P S Q " f [^
 P T Q d q f [∞

y } E



y } Z

ブロック暗号の例



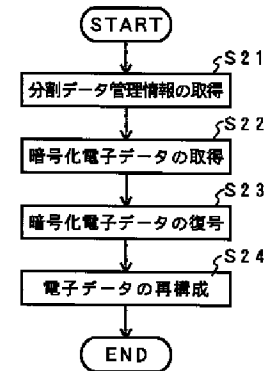
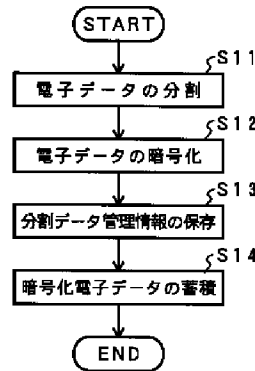
P U Q d q f [^
 P V Q d q f [〃
 P W Q " f [〃
 P X Q ^ » d Q

y } Q

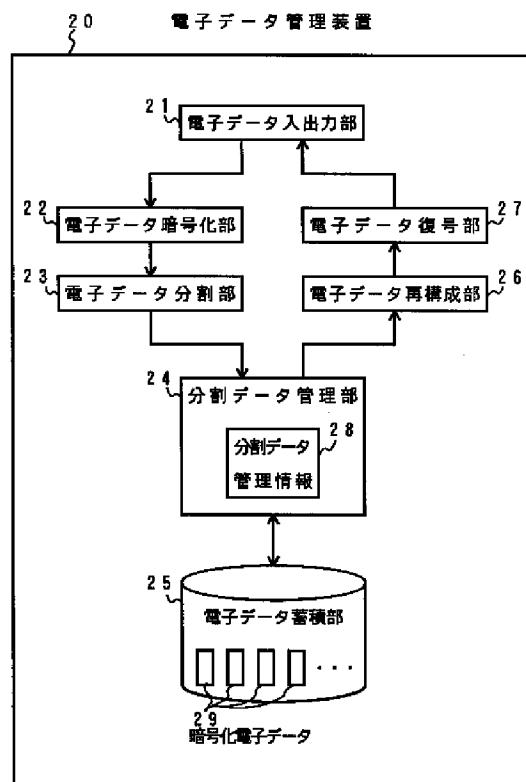
y } R

電子データ蓄積処理の処理フロー

電子データ取得処理の処理フロー



y } S



y } ㉔

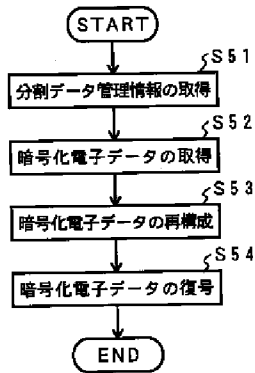
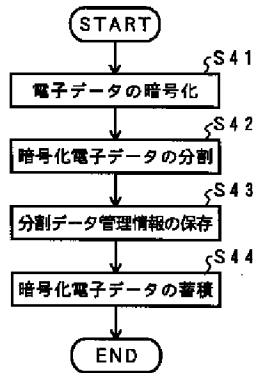
y } ㉕

y } ㉖

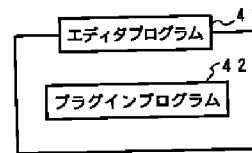
電子データ蓄積処理の処理フロー

電子データ取得処理の処理フロー

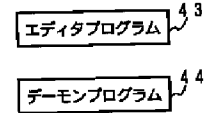
アプリケーションとの連携の例



(A) プラグイン方式



(B) デモンプログラム方式



y } ㉗

分割ファイル保存時の名称の例

絶対パスを用いた分割ファイル名表記	/home/data1/xyz, /home/data2/qwe, ...
ネットワーク上に保存する場合	http://www.foo1.ne.jp/data3/xyz, ftp://ftp.foo2.ne.jp/data4/qwe

y } ㉘

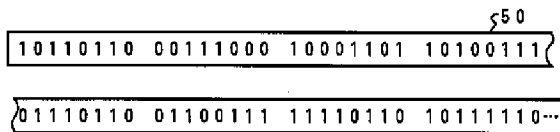
分割データ管理情報（ファイル管理テーブル）の例

ファイル名	暗号鍵	分割数	分割ファイル名
aaa.doc	asdfg	7	xyz, qwe, asf, ...
bbb.txt	zxcvb	56	qaz, wsx, edc, ...
⋮	⋮	⋮	⋮

y } ㉙

文字データビット列の変換による暗号化

(A)



(B)



t g y W

(72)	>	n		æ			e	^	[Q	j5B017 AA07 BA07 BB02 CA16
			s	V	h	9	Q	æ	{		5B065 BA00 PA04 PA16
		d	M	d	b	#					5B082 GA02 GA11
(72)	>]	"	o							5J104 AA12 JA03 JA07 NA02 NA30
			s	V	h	9	Q	æ	{		PA14
		d	M	d	b	#					